



US006149522A

United States Patent [19]

Alcorn et al.

[11] Patent Number: 6,149,522

[45] Date of Patent: *Nov. 21, 2000

[54] **METHOD OF AUTHENTICATING GAME DATA SETS IN AN ELECTRONIC CASINO GAMING SYSTEM**

[75] Inventors: Allan E. Alcorn, Portola Valley; Michael Barnett, Santa Clara; Louis D. Giacalone, Jr., Palo Alto; Adam E. Levinthal, Redwood City, all of Calif.

[73] Assignee: Silicon Gaming - Nevada, Las Vegas, Nev.

[*] Notice: This patent is subject to a terminal disclaimer.

[21] Appl. No.: 09/107,031

[22] Filed: Jun. 29, 1998

Related U.S. Application Data

[63] Continuation-in-part of application No. 08/981,882, filed as application No. PCT/US96/10463, Jun. 17, 1996, which is a continuation-in-part of application No. 08/497,662, Jun. 29, 1995, Pat. No. 5,643,086.

[51] Int. Cl.⁷ G06F 5/00

[52] U.S. Cl. 463/29; 380/25

[58] Field of Search 380/28, 4, 9, 23, 380/30, 49, 50, 59; 463/29, 16, 40, 41, 42, 44

Primary Examiner—Valencia Martin-Wallace

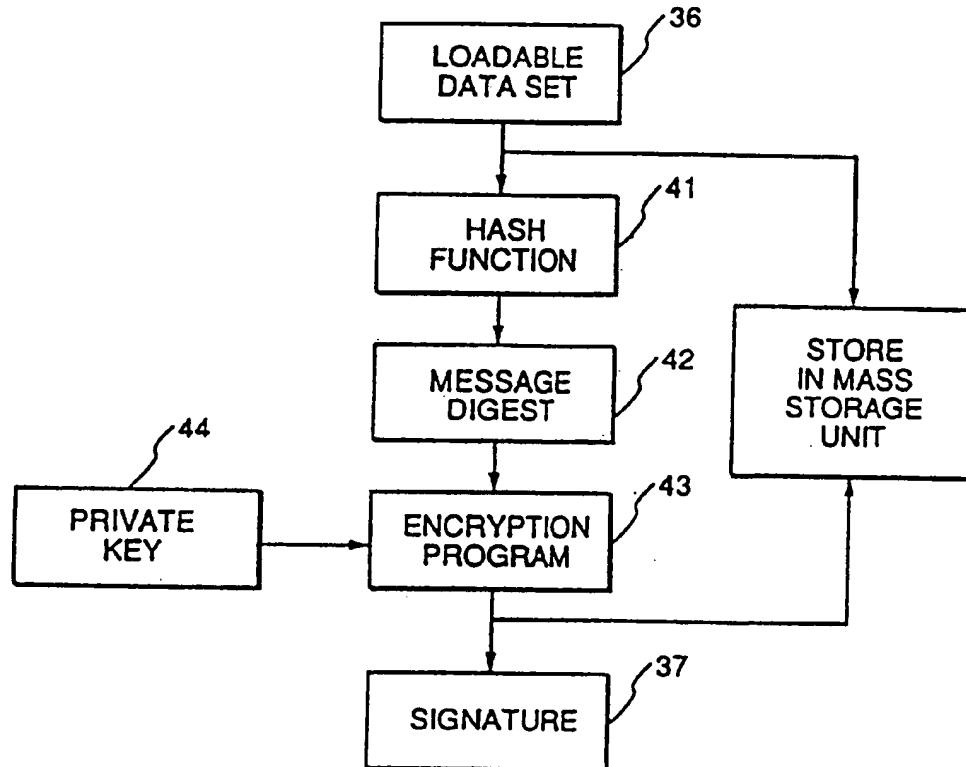
Assistant Examiner—John Paradiso

Attorney, Agent, or Firm—Claude A. S. Hamrick; Justin Boyce; Oppenheimer Wolff & Donnelly LLP

[57] ABSTRACT

Authentication of a casino game data set is carried out within the casino game console using an authentication program stored in an unalterable ROM physically located within the casino game console. The casino game data set and a unique signature are stored in a mass storage device, which may comprise a read only unit or a read/write unit and which may be physically located either within the casino game console or remotely located and linked to the casino game console over a suitable network. The authentication program stored in the unalterable ROM performs an authentication check on the casino game data set at appropriate times, such as prior to commencement of game play, at periodic intervals or upon demand. At appropriate occasions, the contents of the unalterable ROM can be verified by computing the message digest of the unalterable ROM contents and comparing this computed message digest with a securely stored copy of the message digest computed from the ROM contents prior to installation in the casino game console.

49 Claims, 4 Drawing Sheets



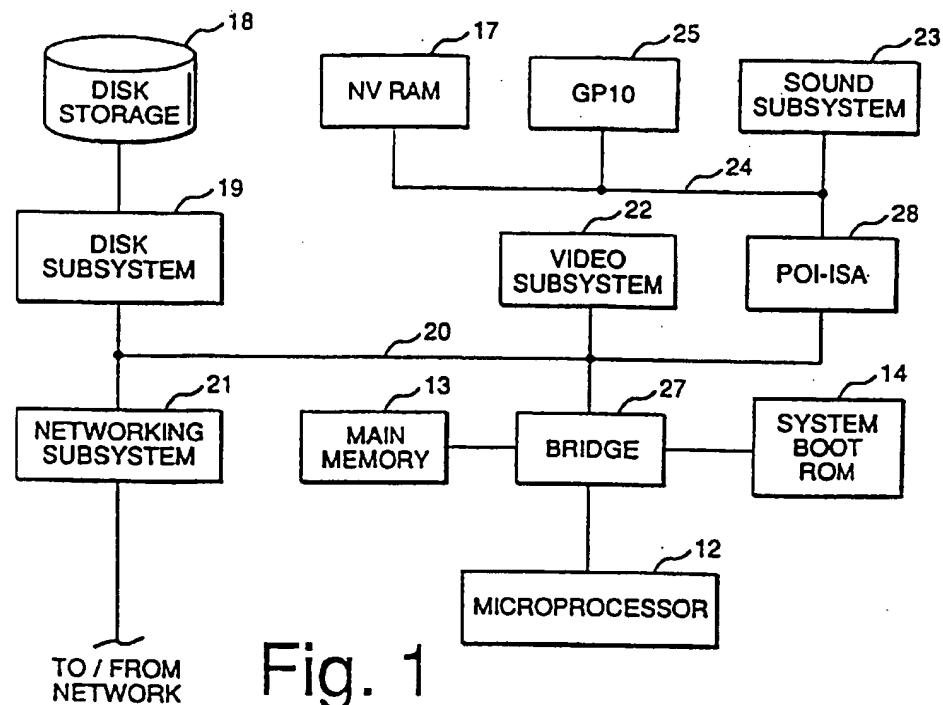


Fig. 1

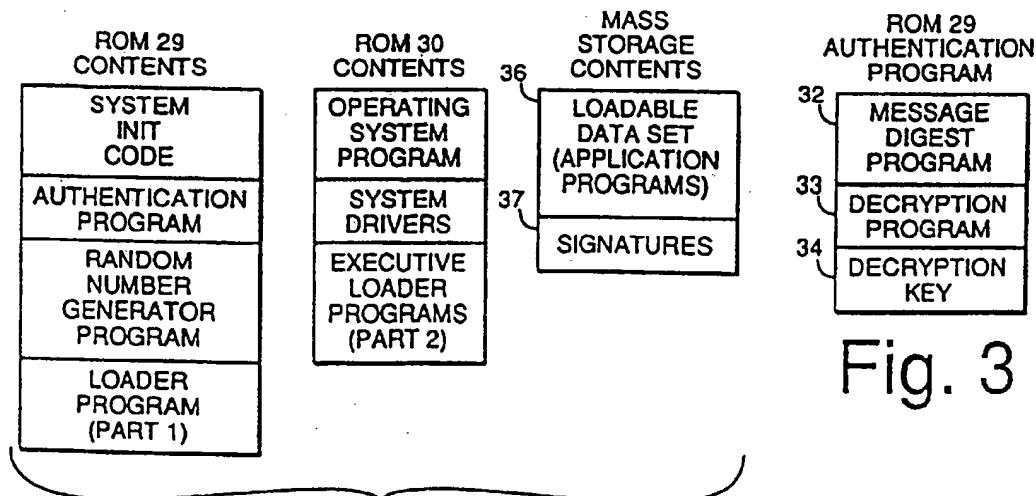
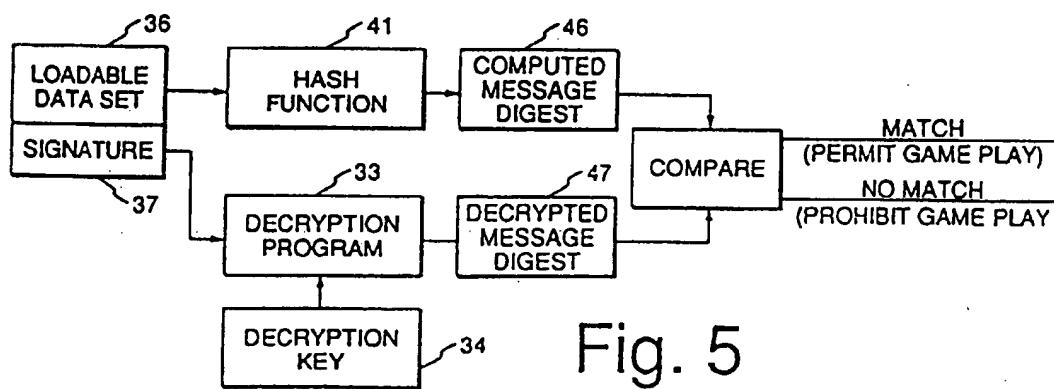
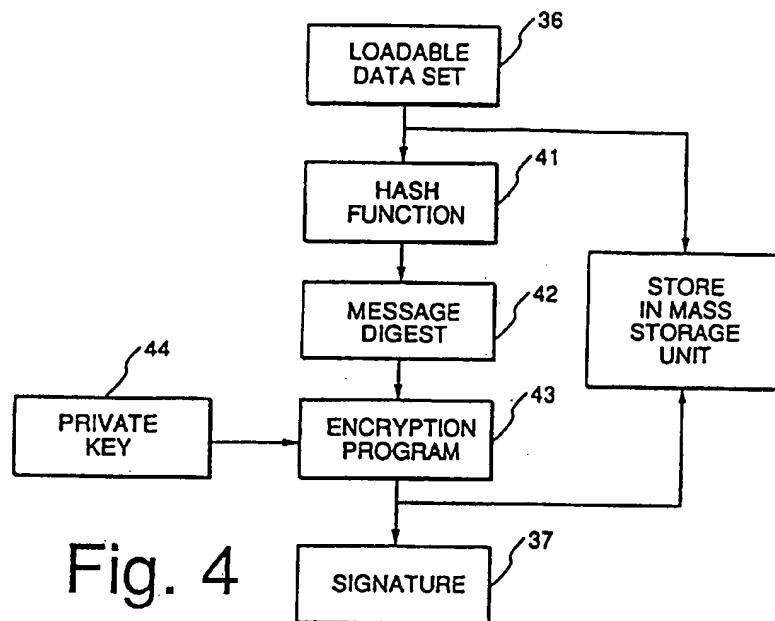


Fig. 2

Fig. 3



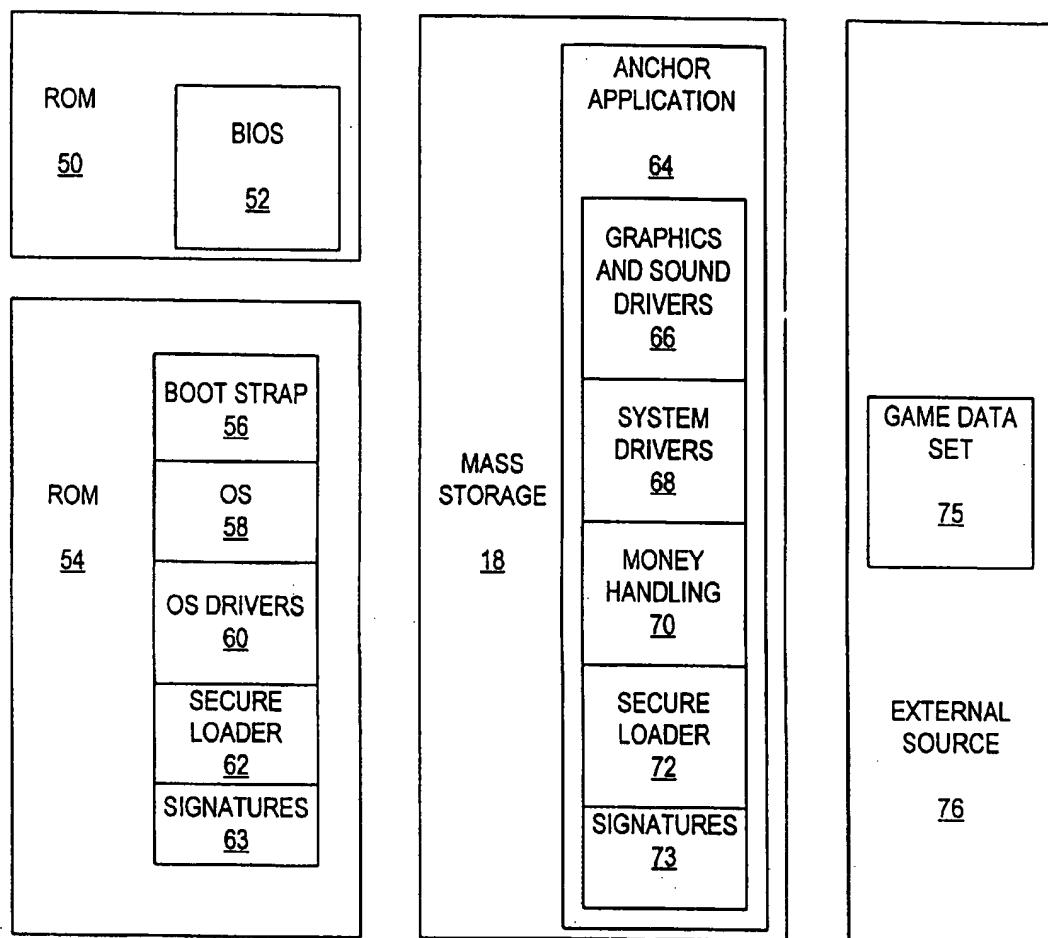


FIG. 6

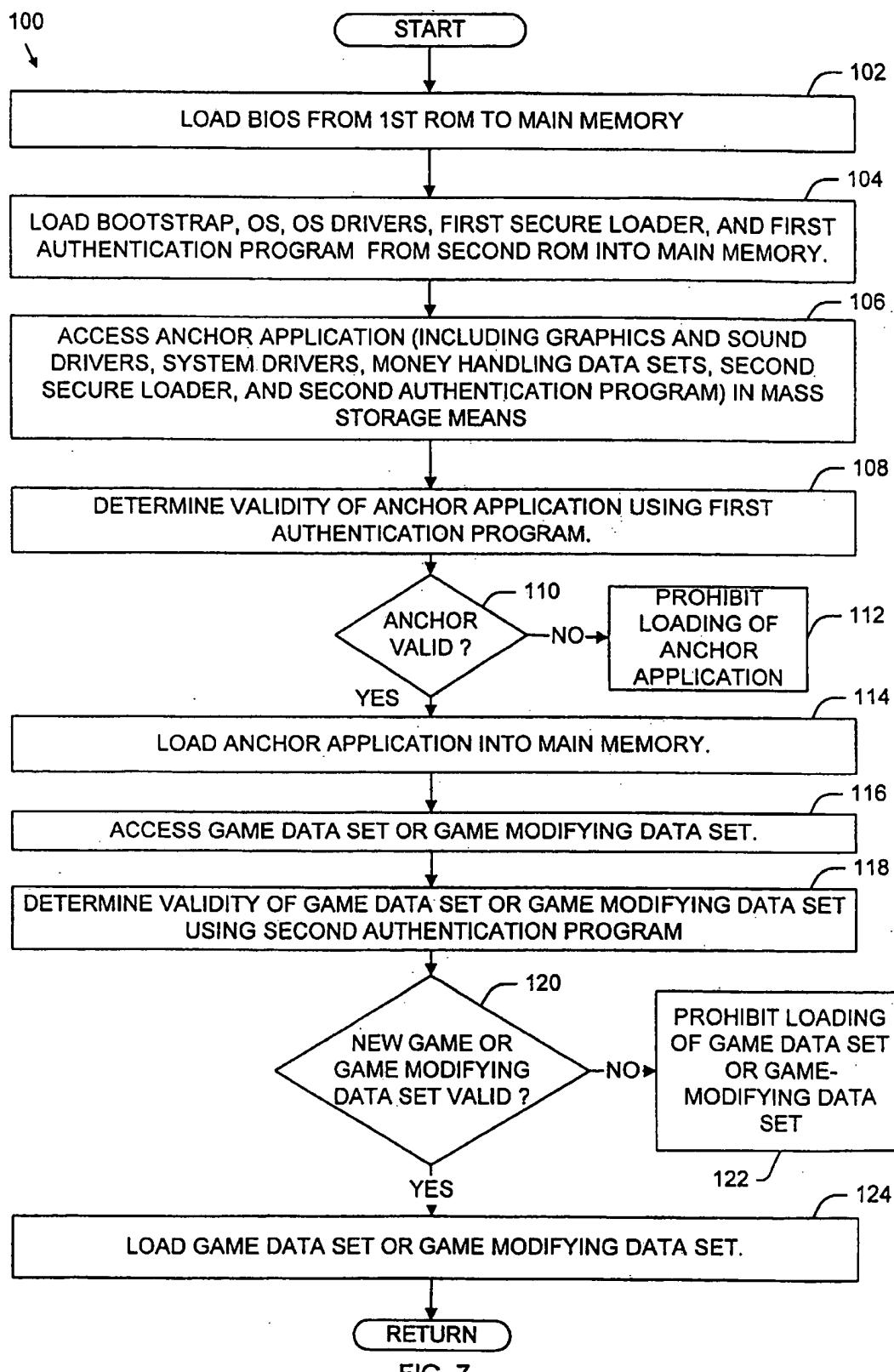


FIG. 7

**METHOD OF AUTHENTICATING GAME
DATA SETS IN AN ELECTRONIC CASINO
GAMING SYSTEM**

**CROSS REFERENCE TO RELATED
APPLICATIONS**

This application is a continuation-in-part of U.S. patent application, Ser. No. 08/981,882, filed Dec. 29, 1997 and entitled "Electronic Casino Gaming System With Improved Play Capacity, Authentication and Security" (U.S. National phase application of PCT application Ser. No. PCT/US96/10463, filed June 17, 1996), which is a continuation-in-part of U.S. patent application, Ser. No. 08/497,662, filed Jun. 29, 1995, and entitled "Electronic Casino Gaming Apparatus With Improved Play Capacity, Authentication and Security", now U.S. Pat. No. 5,643,086.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to microprocessor based gaming systems used in gambling casinos, and more particularly to a method of authenticating game data sets in an electronic gaming system.

2. Brief Description of the Prior Art

Microprocessor based gaming systems are known which are used in gambling casinos to augment the traditional slot machine games (e.g. three reel single or multi-line games) and card games, such as poker and black jack. In a typical gaming system of this type, a microprocessor based system includes both hardware and software components to provide the game playing capabilities. The hardware components include a video display for displaying the game play, mechanical switches for enabling player selection of additional cards or game play choices, coin acceptors and detectors and the electronic components usually found in a microprocessor based system, such as random access memory (RAM), read only memory (ROM), a processor and one or more busses. The software components include the initialization software, credit and payout routines, the game image and rules data set, and a random number generator algorithm. In order to be acceptable for casino use, an electronic gaming system must provide both security and authentication for the software components. For this reason, gaming commissions have heretofore required that all software components of an electronic gaming system be stored in unalterable memory, which is typically an unalterable ROM. In addition, a copy of the contents of the ROM or a message digest of the contents (or both) are normally kept on file in a secure location designated by the gaming commission so that the contents of an individual ROM removed from a gaming machine can be verified against the custodial version.

In a typical arrangement, a message digest of the ROM contents is initially generated prior to the installation of the ROM in the machine by using a known algorithm usually referred to as a hash function. A hash function is a computation procedure that produces a fixed-size string of bits from a variable-size digital input. The fixed-sized string of bits is termed the hash value. If the hash function is difficult to invert—termed a one-way hash function—the hash function is also termed a message digest function, and the result is termed the message digest. The message digest is unique to any given variable size input data set, i.e., the game data set stored in the ROM. When it becomes necessary to later authenticate the ROM from any given machine, the ROM is physically removed from the game console and the message

digest of the ROM contents is computed directly from the ROM using the original hash function. The computed message digest is compared with the message digest on file at the designated custodial location (typically in the casino itself).

5 This procedure is typically carried out whenever a machine produces a payoff beyond a given threshold value. If the two message digests match, then the contents of the ROM are considered to be authenticated (verified) and the payout is made to the player.

10 While such electronic casino gaming systems have been found to be useful in promoting casino game play, the restriction requiring that the casino game program be stored in unalterable ROM memory, leads to a number of disadvantageous limitations. First, due to the limited capacity of the ROM storage media traditionally used to hold the program, the scope of game play available with such systems is severely limited. For sophisticated games using motion video and audio multi-media elements, much more memory capacity, on the order of hundreds of megabytes, is

15 necessary. However, physical verification of such a large quantity of physical devices is not practical, and has thus far been an impediment to creating sophisticated games with more player appeal. Second, the authentication check is only conducted on a limited basis (usually after a jackpot) or

20 other significant winning game outcome, and the authentication procedure requires that game play be halted until the ROM contents have been found to be authentic. These limitations make it very difficult to modify game parameters, such as the game rules or the payout scheme of the game

25 being played on the gaming system. It would be advantageous to be able to modify the game parameters of a game

30 currently being played on a game system without requiring physical verification of new games or game modifying data sets.

35

SUMMARY OF THE INVENTION

The invention comprises an electronic casino gaming system which greatly expands casino game play capability and enhances security and authentication capabilities. More particularly, the invention comprises an electronic casino gaming system and method having greatly expanded mass storage capability for storing a multiplicity of high resolution, high sound quality casino type games, and provides enhanced authentication of the stored game program information with a high security factor.

According to a first aspect of the invention, authentication of a casino game data set is carried out within the casino game console using an authentication program stored in an unalterable ROM physically located within the casino game console.

50 The casino game data set and a unique signature are stored in a mass storage device, which may comprise a read only unit or a read/write unit and which may be physically located either within the casino game console or remotely located and linked to the casino game console over a suitable network. The authentication program stored in the unalterable ROM performs an authentication check on the casino game data set at appropriate times, such as prior to commencement of game play, at periodic intervals or upon demand. At appropriate occasions, the contents of the unalterable ROM can be verified by computing the message digest of the unalterable ROM contents and comparing this computed message digest with a securely stored copy of the message digest computed from the ROM contents prior to installation in the casino game console.

55 60 65 From a process standpoint, this aspect of the invention comprises a method of authenticating a data set of a casino

style game which consists of two phases: a game data set preparation phase and a game data set checking phase. In the game data set preparation phase, the method proceeds by providing a data set for a casino game, computing a first abbreviated bit string unique to the casino game data set, encrypting the first abbreviated bit string to provide an encrypted signature of the casino game data set, and storing the casino game data set and the signature in a mass storage device. The first abbreviated bit string is preferably computed using a hash function to produce a message digest of the casino game data set. The signature is then generated by encrypting the message digest. After storage of the game data set and unique signature, this information is installed in a casino game console. The casino game data set checking phase proceeds by computing a second abbreviated bit string from the stored casino game data set using the same hash function, decrypting the stored encrypted signature to recover the first abbreviated bit string, and comparing the first and second abbreviated bit strings to determine whether the two strings match. If a match does occur, the casino game data set is deemed authentic; if there is no match, authentication is denied and game play is prohibited.

The encryption/decryption process is preferably performed using a private key/public key technique in which the first abbreviated bit string is encrypted by the game manufacturer using a private encryption key maintained in the custody of the game manufacturer. The decryption of the signature is performed using a public key which is contained in an unalterable read only memory element located in the game console, along with the casino game data set. The casino game data set is preferably stored in a mass storage device, such as a magnetic or CD-ROM disk drive unit or a network file unit, the selected unit having a relatively large capacity. The actual size of the mass storage device will depend upon the casino game storage requirements and can be tailored to any specific application.

Each time a casino game data set is transferred from the mass storage device to the main memory of the system, the authentication routine is run. The authentication routine can also be activated by means of an operator switch mounted in the game console or remotely via a network. Consequently, the authenticity of the data set can be automatically checked whenever the transfer occurs and at other appropriate times.

In order to detect attempts to tamper with the contents of the unalterable read only memory element located in the game console, a message digest computed for the authentication program stored therein is stored in a secure manner in a different location from the game console, such as the casino operator's security facilities or the facilities of a gaming commission (or both). The authenticity of the unalterable read only memory element is checked in the same way as that now performed in prior art devices: viz. computing the message digest directly from the unalterable read only memory device, and comparing the message digest thus computed with the custodial version.

From an apparatus standpoint, the first aspect of the invention comprises an electronic casino gaming system having means for providing authentication of a game data set of a casino type game prior to permitting game play, the system including first means for storing a casino game data set and a signature of the casino game data set, the signature comprising an encrypted version of a unique first abbreviated bit string computed from the casino game data set; second means for storing an authentication program capable of computing a second abbreviated bit string from the casino game data set stored in the first storing means and capable of decrypting the encrypted signature stored in the first

storing means to recover the first abbreviated bit string; processing means for enabling the authentication program to compute an abbreviated bit string from the casino game data set stored in the first storing means and for enabling the authentication program to decrypt the encrypted signature; and means for comparing the computed second abbreviated bit string with the decrypted abbreviated bit string to determine whether a match is present. The first storing means preferably comprises a mass storage device, such as a disk drive unit, a CD-ROM unit or a network storage unit. The second storing means preferably comprises an unalterable read only memory in which the authentication program is stored.

According to a second aspect of the invention, the authentication program stored in the unalterable ROM located within the casino game console is used to test the authenticity of all other programs and fixed data stored in memory devices in the electronic casino gaming system, such as a system boot ROM, memory devices containing the operating system program, system drivers and executive/loader programs, and other memory devices incorporated into the electronic casino game system architecture. The contents of each such memory device, whether program information or fixed data, include signatures encrypted from message digests computed using a hash function from the original program information or fixed data set. Upon system initialization, the authentication program in the unalterable ROM is used to authenticate the individual memory device contents in essentially the same fashion as that used to authenticate the casino game data sets. More specifically, the message digest for the given program or fixed data set is computed using the same hash function originally used to produce the message digest for that program or fixed data set. The encrypted signature is decrypted using the proper decryption program and decryption key to recover the message digest. The two versions of the message digest are then compared and, if found to be matching, the concerned program or fixed data set is deemed authentic and is permitted to be used by the system. Once all of the concerned programs and fixed data sets have been so authenticated, the casino game data set authentication procedure is run, after which game play is permitted (provided a match occurs).

From a process standpoint, this second aspect of the invention comprises a method of authenticating a program or data set of a casino style game which consists of two phases: a program or fixed data set preparation phase, and a program or fixed data set checking phase. In the program or fixed data set preparation phase, the method proceeds by providing a program or fixed data set for a casino game, computing a first abbreviated bit string unique to the program or fixed data set, encrypting the first abbreviated bit string to provide an encrypted signature of the program or fixed data set, and storing the program or fixed data set and the signature in a memory device. The first abbreviated bit string is preferably computed using a hash function to produce a message digest of the program or fixed data set. The signature is then encrypted from the message digest. After storage of the program or fixed data set and unique signature in the memory device, the memory device is installed in a casino game console. The casino game program or fixed data set checking phase proceeds by computing a second abbreviated bit string from the stored casino game program or fixed data set stored in the memory device using the same hash function, decrypting the encrypted signature stored in the memory device to recover the first abbreviated bit string, and comparing the first and second abbreviated bit strings to determine whether the two strings

match. If a match does occur, the casino game program or fixed data set is deemed authentic; if there is no match, authentication is denied and use of that casino game program or fixed data set is prohibited.

The authentication routine is run each time a given casino game program or fixed data set needs to be called or used. The authentication routine can also be run automatically on a periodic basis, or on demand—either locally by means of an operator switch mounted in the casino game console or remotely via a network. Consequently, the authenticity of the casino game program or fixed data set can be automatically checked whenever use of that program or fixed data set is required and at other appropriate times, such as in the course of a gaming commission audit.

The present invention also provides a two-stage method of authenticating game data sets for implementing casino-type games in an electronic gaming system including a main memory, a first storage means having a first authentication program stored therein, a second storage means having stored therein an anchor application including a second authentication program, and an anchor signature including an encrypted version of a unique primary abbreviated anchor bit string computed from the anchor application, and a third storage means having stored therein a game data set and a game signature including an encrypted version of a unique primary abbreviated game bit string computed from the game data set.

The first authentication program stored in the first storage means is loaded to the main memory. The anchor application stored in the second storage means is accessed. The validity of the anchor application is determined using the first authentication program. If the anchor application is invalid, then loading of the anchor application into the main memory is prohibited. If the anchor application is valid, then the anchor application is loaded into the main memory, the game data set stored in the third storage means is accessed, and the validity of the game data set is determined using the second authentication program. If the game data set is invalid, then loading of the game data set into the main memory is prohibited. If the game data set is valid, then the game data set is loaded into the main memory and instructions of the game data set are processed.

In a preferred embodiment, the step of determining the validity of the anchor application using the first authentication program includes the steps of: computing a complementary abbreviated anchor bit string from the anchor application; decrypting the anchor signature to recover the primary abbreviated anchor bit string; and comparing the primary and complementary abbreviated anchor bit strings to determine whether the primary and complementary abbreviated anchor bit strings match. Also in the preferred embodiment, the step of determining the validity of the game data set using the second authentication program includes the steps of: computing a complementary abbreviated game bit string from the game data set; decrypting the game signature to recover the primary abbreviated game bit string; and comparing the primary and complementary abbreviated game bit strings to determine whether the primary and complementary abbreviated game bit strings match.

The electronic gaming system further includes a fourth storage means having stored therein a basic input/output operating system (BIOS). The first storage means includes bootstrap code, an operating system, and operating system drivers stored therein. Initially, the BIOS is loaded from the fourth storage means to the main memory; and then the

bootstrap code, operating system, and operating system drivers are loaded from the first storage means to the main memory.

Electronic casino game systems incorporating the invention provide a vastly expanded capacity for more sophisticated and attractive casino-style games, while at the same time improving the authentication of the games without compromising security. In addition, casino game systems incorporating the invention provide great flexibility in changing casino game play, since the casino game data sets representing the various games can be stored in alterable media rather than read only memory units as with present casino game systems.

By separating the authentication process from the casino game data set storage, the invention affords secure distribution and execution of program code and data, regardless of the particular distribution or storage technique employed. More specifically, the invention allows the casino game data set to reside in any form of secondary storage media, such as the traditional ROM storage, hard magnetic disk drives and CD-ROM drives, or networked file systems. So long as the authentication procedure conducted on the game data set is performed using the authentication program stored in an unalterable ROM, and so long as that ROM can be verified reliably, any casino game data set can be loaded from any source and can be verified by the system at any time: either prior to use, during run-time, periodically during run-time or upon demand. The large quantities of storage that can be made available in a secure fashion using the invention, facilitates the creation of casino gaming systems offering both an increased diversity of games, and individual games of superior quality. In addition, the authentication of all casino game program and fixed data software ensures the integrity of all system software both prior to game play and thereafter at periodic or random intervals.

For a fuller understanding of the nature and advantages of the invention, reference should be had to the ensuing detailed description taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a system incorporating the invention;

FIG. 2 is a schematic diagram illustrating the contents of the read only memory and the mass storage device;

FIG. 3 is a more detailed schematic view of the authentication program stored in the ROM and the game data stored in the mass storage unit;

FIG. 4 is a diagram illustrating the preparation of the game data set;

FIG. 5 is a diagram illustrating the authentication procedure for the game data set;

FIG. 6 is a diagram illustrating an alternative approach to the secure loading of software into the system; and

FIG. 7 is a flow diagram illustrating a two stage authentication process according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Turning now to the drawings, FIG. 1 is a block diagram of an electronic casino gaming system incorporating the invention. As seen in this figure, the system consists of several system components under software control. These system components include a microprocessor 12, which may comprise any general purpose microprocessor, such as a

Pentium-based microprocessor from Intel Corporation. A main memory unit 13 is provided, which is typically a random access memory having a capacity of between 32 and 64 megabytes for storing the majority of programs and graphics elements during game play. A system boot ROM 14 provides the initialization software required when power is first applied to the system. ROM 14 contains additional programs in read only form, including the operating system, related drivers and the authentication software described in detail below. A non-volatile RAM 17 is a battery backed static RAM capable of maintaining its contents through power cycling. NV RAM 17 stores significant information relating to game play, such as the number of player credits, the last game outcome and certain diagnostic and error information not critical to an understanding of the invention.

A mass storage unit implemented in the FIG. 1 system as a magnetic hard disk drive unit 18 is coupled to and controlled by a disk subsystem 19 of conventional design and operation. Disk drive unit 18 provides storage for the game specific data set, which includes both program data and image data specifying the rules of the various different casino games or single casino game variations, and the types of images and image sequences to be displayed to the game players. The size of the disk drive unit 18 is a function of the number of games and game variations provided for a given system, as well as the amount of data required for each specific game. In general, the more motion video designed into a particular casino game, the more storage required for that casino game software. A disk drive unit 18 with a 4-gigabyte capacity will usually provide sufficient storage capacity. Disk subsystem 19 comprises a disk controller connected to a PCI bus 20 for controlling the disk drive unit 18. Controller 19 preferably supports SCSI-2, with options of fast and wide. It should be noted that a number of different types of locally-based disk drive units may be used in the FIG. 1 system, including a CD-ROM storage unit. Also, the mass storage unit need not be physically located within the game console along with the other elements depicted in FIG. 1: the mass storage unit may be located remotely from the game console and coupled thereto by means of an appropriate network, such as an Ethernet, an RS232 link, or some other hard-wired or wireless network link. This latter alternate arrangement is indicated by the inclusion of a network subsystem 21 of appropriate configuration and functional characteristics, which may have Ethernet, RS232 serial, or other network compatibility.

A video subsystem 22 is coupled to the PCI bus and provides the capability of displaying full color still images and MPEG movies with a relatively high frame rate (e.g. 30 frames per second) on an appropriate monitor (not shown). Optional 3D texture mapping may be added to this system, if desired.

A sound subsystem 23 having a stereo sound playback capability with up to 16 bit CD quality sound is coupled to an ISA bus 24. A general purpose input/output unit 25 provides interfaces to the game mechanical devices (not illustrated) such as manually actuated switches and display lights. A first bridge circuit 27 provides an interface between microprocessor 12, ROM 14, main memory 13 and PCI bus 20. Bridge circuit 27 is preferably a TRITON chip set available from INTEL Corporation. A second bridge circuit 28 provides an interface between the PCI bus 20 and the ISA bus 24. Bridge circuit 28 is preferably a type 82378 chip available from Intel Corporation.

FIG. 2 illustrates the types of information stored in the system ROM 14 and the mass storage unit. As seen in FIG. 2, the ROM unit 14 used in the FIG. 1 system comprises two

separate ROM elements: ROM 29 and ROM 30. ROM 29 must be an unalterable device, such as a Toshiba type C53400 512Kx8 bit mask programmed ROM. ROM 30 is preferably an unalterable device like ROM 29, but may comprise a different type of ROM, such as a type 29OF40 field programmable flash ROM available from Intel Corp. ROM 29 contains the system initialization or boot code, an authentication program, and an initial portion of the executive/loader programs. ROM 30 contains the operating system program, the system drivers and the remainder of the executive/loader programs as noted below. The mass storage unit contains the applications, which include the game image and sound data, rules of game play and the like, and the signature associated with each particular casino game.

FIG. 3 illustrates the authentication and application program information in more detail. As seen in this figure, the authentication program stored in unalterable ROM 29 comprises a message digest algorithm component 32, a decryption algorithm component 33, and a decryption key component 34. The message digest algorithm component 32 stored in ROM 29 comprises an exact copy of a hash function program routine used to originally compute a message digest from the loadable game data set 36 in a manner described below. The decryption algorithm component 33 stored in ROM 29 comprises the algorithm required to decrypt any encrypted casino game data set signature using the decryption key component 34.

The decryption key component 34 comprises the decryption key that is required to decrypt any of the encrypted signatures 37 in the manner described below during the authentication routine.

FIG. 4 illustrates the manner in which an encrypted data set signature 37 is generated. A loadable casino game data set 36 is processed using a hash function 41 to generate a message digest 42 which is unique to the loadable game data set 36. The hash function employed may be one of a number of known hash functions, such as the MD2, MD4, and MD5 hash functions and the SHA hash function; or any other suitable hash function capable of producing a unique abbreviated bit string from a variable size input data set. For further information about these hash functions, reference should be had to the publication entitled "Answers To Frequently Asked Questions About Today's Cryptography", Revision 2.0, Oct. 5, 1993, published by RSA Laboratories, Redwood City, Calif., and the publications listed in the references section thereof, the disclosures of which are hereby incorporated by reference. After generation, the message digest 42 is then encrypted with an encryption algorithm 43 using a private encryption key 44 to generate a signature 37 of the message digest. In the preferred embodiment, the two-key (private/public key) encryption technique developed by RSA Data Security, Inc., of Redwood City, Calif., is used. This technique is disclosed and described in U.S. Pat. Nos. 4,200,770, 4,218,582 and 4,405,829, the disclosures of which are hereby incorporated by reference. The signature 37 of the message digest 42 is then stored in the mass storage unit along with the loadable data set 36.

FIG. 5 illustrates the authentication routine carried out in accordance with the invention. When the authentication routine is called (see below), the loadable casino game data set 36 is transferred from the mass storage unit to main memory 13 (unless already there), and the message digest of casino game data set 36 is computed using the message digest algorithm 32. The message digest algorithm uses the same hash function 41 as that used by the manufacturer to prepare the original message digest 42 (FIG. 4). The result

is an unencrypted version 46 of the message digest computed from the casino game data set 36 currently present in the mass storage unit. The encrypted data set signature 37 is decrypted using the public decryption key 34 matching the private key 44 used to originally encrypt the message digest 42 of the casino game data set 36. The message digest 47 decrypted with decryption key 34 is then compared with the message digest 46 computed from the casino game data set 36. If the two message digests match, then the casino game data set 36 is deemed authentic and game play may proceed. If there is no match, either the casino game data set 36 or the signature 37 is deemed corrupted and not authentic. Game play is prohibited and appropriate actions can be taken: e.g., alerting a security employee using a suitable messaging system (an audible alarm, flashing lights, or a network message from the game console to a central security area).

Since authentication of the game data set 36 and signature 37 (FIG. 2) is entrusted to the contents of ROM 29 (FIG. 2), a procedure must be provided to verify the ROM 29 contents. For this purpose, a message digest is computed for the authentication program stored in ROM 29, and this message digest is stored in a secure manner with the casino operator or the gaming commission (or both) along with the hash function used to produce the message digest. This hash function may be the same hash function used to compute the message digest 42 of the casino game data set or a different hash function. In this way, the authenticity of the ROM 29 can be easily checked in the same way as that now performed in prior art devices: viz. computing the message digest directly from the ROM 29 and comparing the message digest thus computed with the custodial version of the message digest. If required by a given gaming commission or deemed desirable by a casino operator, the system may also display the message digest 42 of each particular data set 36 or the encrypted signature version 37 for auditing purposes. In addition, the system may transmit this information via networking subsystem 21 to an on-site or off-site remote location (such as the office of the gaming commission). The message digest displayed or transmitted may comprise the decrypted version or the computed version (or both).

The authentication procedure carried out by means of the message digest program 32, decryption program 33 and decryption key 34 stored in unalterable ROM 29 in the manner described above is also used to authenticate the contents of all memory devices in the FIG. 1 system, such as the contents of ROM 30 (see FIG. 2), the fixed data portions and program components stored in NV RAM 17 and the program and fixed data contents of any memory devices stored in the networking subsystem 21, video subsystem 22, sound subsystem 23, PCI-ISA interface 24, and GPIO unit 25. Each program or fixed data set stored in any memory device in any of these units has an associated signature, which is encrypted from a message digest of the original program or fixed data set using a hash function, which is preferably the same hash function used to prepare the message digest of the casino game data set. Prior to permitting any such program or fixed data set to participate in the system operation, that program or fixed data set is subjected to the authorization procedure to ensure that the message digest computed from the current version of the program or fixed data set matches the message digest decrypted from the encrypted signature associated to the program or fixed data set. In addition, the authentication procedure can be run on each such program or fixed data set at periodic or random intervals (on demand) in a manner essentially identical to that described above with respect to the casino game data set authentication procedure. As a

consequence, the integrity of all software in the system is checked prior to the use of that particular software in order to reveal any unauthorized changes to the software portion of the casino gaming system.

An alternative approach to the secure loading of software into the system is depicted in FIG. 6. In this embodiment, basic input/output system (BIOS) software 52 is stored in a ROM 50, the first of two ROMs 50 and 54 making up the system boot ROM 14 (FIG. 1). The second ROM 54 stores boot strap code 56, operating system (OS) code 58, OS drivers 60, and a first secure loader 62 including a first authentication program, and one or more signatures 63 associated with the boot strap code, OS code, OS drivers, and first secure loader. The first authentication program implements the authentication procedure described above in reference to FIG. 5.

In the preferred embodiment, each of the signatures 63 includes an encrypted version of a unique primary abbreviated bit string, and is determined as described above in FIG. 4. Signatures 63 may include a single signature calculated from all data sets stored in second ROM 54 or may include a plurality of signatures, each calculated from a single data set, or from a combination of data sets, stored in second ROM 54. In a preferred embodiment, signatures 63 include a first authentication program signature which is an encrypted version of a unique primary abbreviated bit string computed from the first authentication program using the signature generating process described in FIG. 4. In an embodiment, a copy of the contents of second ROM 54 or a message digest of the contents (or both) are kept on file in a secure location so that the contents of the second ROM can be removed from a gaming machine and verified against the custodial version.

An anchor application 64, stored in mass storage 18 (FIG. 3) includes graphics and sound drivers 66, system drivers 68, money-handling software 70, a second secure loader 72, and one or more signatures 73 associated with the drivers 66 and 68, money handling software, and second secure loader. Second secure loader 72 includes a second authentication program which, in the preferred embodiment, implements the authentication procedure described above in FIG. 5. In the preferred embodiment, each of the signatures 73 includes an encrypted version of a unique primary abbreviated bit string, and is determined as described above in FIG. 4. Signatures 73 may include a single signature calculated from all data sets of the anchor application or may include a plurality of signatures, each calculated from a single data set, or from a combination of data sets, of the anchor application. In one embodiment of the present invention, signatures 63 are computed using a first hash function while signatures 73 are computed using a second dissimilar hash function, and the first and second authentication programs authenticate data sets using the first and second hash functions respectively.

In an embodiment, anchor application signatures 73 include: a second authentication signature including an encrypted version of a unique primary abbreviated bit string computed from the second authentication program; a graphics and sound driver signature including an encrypted version of a unique primary abbreviated bit string computed from graphics and sound drivers 66; system driver signatures including encrypted versions of a unique primary abbreviated bit strings computed from system drivers 68; and a money handling signature including an encrypted version of a unique primary abbreviated bit string computed from money-handling software 70. In an alternative embodiment, a single anchor signature including an

encrypted version of a unique primary abbreviated bit string computed from all data sets of anchor application 64 is used.

The second authentication program of the anchor application 64 may be used to load an initial game data set for implementing a casino-type game, a new game data set for implementing new casino-type game replacing previously activated casino-type game, or a game modifying data set for modifying game parameters of a previously activated casino-type game. The game-modifying data sets include game-modifying signatures which are encrypted versions of unique primary abbreviated bit strings computed from the game-modifying data sets. The new games include new game signatures which are encrypted versions of unique primary abbreviated bit strings computed from the new game data sets.

A game data set 75 may be received, or accessed, from an external source 76. Game data set 75 may be a new game data set or a game-modifying data set. In varying embodiments, external source 76 may be a ROM, a mass storage device, any other computer readable memory of the electronic gaming system (FIG. 1), or a network storage means which is located remotely from the electronic gaming system and which is accessible via a network. In one embodiment, the mass storage device 18 may serve as the external source 76. The second secure loader 72 of the anchor application 64 may be used to determine the authenticity, or validity, of game data set 75 or any other application to be loaded.

When power is initially applied to the gaming system (FIG. 1) on start-up, or when the system experiences a warm restart, the CPU 12 (FIG. 1) will begin executing code from the BIOS 52 which is responsible for initializing the motherboard and peripheral cards of the system. After BIOS 52 has completed the initialization function, the boot strap code 56 is executed by the CPU 12 (FIG. 1) causing OS 58, OS drivers 60, first secure loader 62, and signatures 63 associated with the OS, OS drivers, and first secure loader to be copied into main memory 13 (FIG. 1). Once in main memory, the OS 58 is started and first secure loader 62 is used to load anchor application 64 from mass storage 18 to main memory 13 as previously indicated.

The anchor application signatures 73 are used during the load by the first authentication program of the first secure loader 62 to verify the validity of the anchor application. After the anchor application 64 is validated, it is used to load all other applications.

The present invention affords great flexibility in game content, scheduling and changes. For example, to change the graphic images in a particular casino game or set of games, new casino game data sets can be generated along with new signatures and stored in the mass storage unit by either exchanging disk drives, replacing disks (for read only disk units), or writing new data to the storage media. In the networked mass storage application, these changes can be made to the files controlled by the network file server. Because the casino game data sets must be authenticated according to the authentication procedure described above in reference to FIG. 5, either periodically or on demand, corrupted data sets cannot go undetected. Thus the invention opens up the field of electronic casino gaming systems to readily modifiable games with flexible displays and rules, without sacrificing the essential security of such systems.

Changes can also be made to the casino type game by using game-modifying data sets. The game-modifying data sets include: a graphics modifying data set for modifying parameters related to graphically displayed images of the

casino-type game; a money handler modifying data set for modifying parameters related to payout of coins and issuing of credit in the casino-type game; and a sound driver modifying data set for modifying parameters related to sound drivers of said casino-type game.

FIG. 7 shows a flow diagram at 100 illustrating a two stage authentication process according to the present invention for authenticating a game data set. In step 102, BIOS 52 (FIG. 6) is loaded from ROM 50 (FIG. 6) to main memory 13 (FIG. 1) of the electronic gaming system. In step 104, system boot data sets are loaded from ROM 54 (FIG. 6) to the main memory. The system boot data sets include boot strap code 56, OS 58, OS drivers 60, first secure loader 62 including the first authentication program (FIG. 6), and associated signatures 63. As mentioned above, in the preferred embodiment, signatures 63 include a first authentication program signature which is an encrypted version of a unique primary abbreviated bit string computed from the first authentication program using the signature generating process described in FIG. 4.

In step 106, anchor application 64 (FIG. 6) is accessed without being loaded into main memory 13 (FIG. 1) of the electronic gaming system. As mentioned, the anchor application includes graphics and sound drivers 66, system drivers 68, money-handling software 70, second secure loader 72, and associated signatures 73 (FIG. 6). In step 108, the validity of anchor application 64 is determined using the first authentication program of the first secure loader 62 (FIG. 6). In this embodiment, the first authentication program determines the validity of the anchor application 64 using the authentication procedure described in FIG. 5.

It is then determined at 110 whether the anchor application 64 is determined to be authentic, or valid, by the first authentication program. If the anchor application is invalid, or not authentic, the depicted process proceeds to step 112 in which case loading of the anchor application to main memory 13 (FIG. 1) is prohibited. If the anchor application is valid, the depicted process proceeds to step 114 in which the anchor application is loaded from mass storage to main memory of the electronic gaming system. After the anchor application is loaded into main memory, the second authentication program of the anchor application may be used to authenticate any further applications accessed or received from any source before loading the applications into main memory. In step 118, the validity of a game data set or game-modifying data set is determined using the second authentication program of the second secure loader 72 (FIG. 6). In the preferred embodiment of the present invention, the second authentication program 10 determines the validity of the game data set or game modifying data set using the authentication procedure described in to FIG. 5.

It is then determined at 120 whether the game data set or game-modifying data set has been determined to be valid by the second authentication program of the second secure loader 72. If the game data set or game-modifying data set is invalid, loading of the new game data set or game-modifying data set, is prohibited as indicated at 120. If the new game data set or game-modifying data set is valid, the depicted process proceeds to step 124 in which the new game data set or game-modifying data set is loaded into main memory.

An important advantage of the invention not found in prior art systems is the time and manner in which the game data sets can be authenticated. In prior art systems, authentication of the casino game data set is normally only done when a payout lying above a given threshold is required by

the outcome of the game play, and this requires that the game be disabled while the ROM is physically removed and the ROM contents are verified.

The authentication procedures of the present invention can be activated to authenticate a data set at a variety of different times without disabling the game. For example, a game data set can be automatically subjected to an authentication procedure of the present invention each time the game is loaded from the mass storage unit into the main memory 13 as suggested by the flow chart of FIG. 7. Further, if desired, the authentication procedure may be initiated in response to the pull of a slot game handle, the detection of a coin insert, the payout of coins or issuing of credit, or any other detectable event related to game play. The authenticity of a given casino game data set 36 (FIG. 2) can also be checked on demand, either locally at the game console or remotely via a network, by providing a demand procedure. Such a procedure may be initiated, e.g. by providing a manually operable switch in the game console, accessible only to authorized persons, for initiating the authentication routine. Alternatively, the system of FIG. 1 may be configured to respond to a demand command generated remotely (e.g. in a security area in the casino or off-site) and transmitted to the game console over a network to the networking subsystem 21.

Another advantage of the invention lies in the fact that the game data set storage capacity of a system incorporating the invention is not limited by the size of a ROM, but is rather dictated by the size of the mass storage unit or external source. As a consequence, games using high resolution, high motion video and high quality stereo sound can be designed and played on systems incorporating the invention. Also, since the mass storage unit need not be a read-only device, and need not be physically located in the game console, the invention affords great flexibility in game content, scheduling and changes. For example, to change the graphic images in a particular casino game or set of games, new casino game data sets can be generated along with new signatures and stored in the mass storage unit by either exchanging disk drives, replacing disks (for read only disk units), or writing new data to the media. In the networked mass storage application, these changes can be made to the files controlled by the network file server. Since the casino game data sets must pass the authentication procedure test, either periodically or on demand, corrupted data sets cannot go undetected. Thus the invention opens up the field of electronic casino gaming systems to readily modifiable games with flexible displays and rules, without sacrificing the essential security of such systems. In fact, security is greatly enhanced by the ability of the invention to authenticate all game data sets both regularly (for each handle pull) and at any time (on demand), without interfering with regular game play (unless no match occurs between the two forms of message digest).

While the above provides a full and complete disclosure of the preferred embodiments of the invention, various modifications, alternate constructions and equivalents may be employed without departing from the true spirit and scope of the invention. For example, while the RSA public/private key encryption technique is preferred (due to the known advantages of this technique), a single, private key encryption technique may be employed, if desired. In a system using this technique, the single key would be stored in ROM 29 in place of the public key 34. Also, the message digest 42 and signature 37 for a given application 36 need not be computed from the entire casino game data set. For example, for some casino games it may be desirable to

provide a fixed set of rules while permitting future changes in the casino game graphics, sound or both. For such casino games, it may be sufficient to compute the message digest 42 and signature 37 from only the rules portion of the applications program 36. In other cases, it may be desirable or convenient to maintain the casino game video and audio portions constant, while allowing future changes to the rules of game play. For casino games of this category, the message digest 42 and signature 37 may be computed from the graphics and sound portions of the application program 36. It may also be desirable to compute a message digest 42 and signature 37 from a subset of the rules, graphics or sound portions of a given applications program 36, or from some other subset taken from a given applications program 36. Therefore, the above should not be construed as limiting the scope of the invention, which is defined by the appended claims.

What is claimed is:

1. A method of authenticating a game data set for use in a casino-type gaming system, said method comprising the steps of:

- (a) receiving the game data set;
- (b) computing a primary abbreviated bit string unique to the game data set;
- (c) encrypting the abbreviated bit string to provide a signature;
- (d) storing the data set and the signature;
- (e) computing a complementary abbreviated bit string from the stored data set;
- (f) decrypting the stored signature to recover the primary abbreviated bit string;
- (g) comparing the primary and complementary abbreviated bit strings to determine whether the primary and complementary abbreviated bit strings match;
- (h) if the primary and complementary abbreviated bit strings match, indicating that the game data set is authentic; and
- (i) if the primary and complementary abbreviated bit strings do not match, indicating that the game data set is not authentic.

2. A method of authenticating a game data set as recited in claim 1 wherein said step (b) of computing is performed with a hash function to produce a hash value of the game data set, and wherein said primary abbreviated bit string comprises the hash value of the game data set.

3. A method of authenticating a game data set as recited in claim 2 wherein the hash value comprises the message digest of the game data set.

4. A method of authenticating a game data set as recited in claim 1 wherein said step (c) of encrypting is performed using a private encryption key.

5. A method of authenticating a game data set as recited in claim 1 wherein said step (f) of decrypting is performed using a public decryption key.

6. A method of authenticating a game data set as recited in claim 1 wherein said step (c) of encrypting is performed using a private encryption key, and said step (f) of decrypting is performed using a public decryption key.

7. A method of authenticating a game data set as recited in claim 1 wherein said step (e) of computing is performed with a hash function to produce a hash value of the stored game data set, and wherein said complementary abbreviated bit string comprises the hash value of the stored game data set.

8. A method of authenticating a game data set as recited in claim 7 wherein the hash value comprises the message digest of the stored game data set.

9. A method of authenticating a game data set as recited in claim 1 wherein said step (d) of storing includes the step of storing the game data set and the signature in a mass storage device.

10. A method of authenticating a game data set as recited in claim 9 wherein the mass storage device comprises a disk drive unit.

11. A method of authenticating a game data set as recited in claim 9 wherein the mass storage device comprises a CD-ROM unit.

12. A method of authenticating a game data set as recited in claim 9 wherein the mass storage device comprises a network storage system.

13. A method of authenticating a game data set as recited in claim 1 wherein said steps (a)-(d) are performed at a first site, and wherein steps (e)-(g) are performed at a second site.

14. A method of authenticating a game data set as recited in claim 13 wherein the first site comprises a manufacturing facility, and wherein said second site is a gaming facility.

15. A method of authenticating a game data set as recited in claim 1 wherein said game data set is a game-modifying data set for modifying game parameters of a casino type game.

16. A method of authenticating a game data set as recited in claim 15 wherein said game-modifying data set includes a money handler modifying data set for modifying parameters related to payout of coins and issuing of credit in the casino-type game.

17. A method of authenticating a game data set as recited in claim 15 wherein said game-modifying data set includes a sound driver modifying data set for modifying parameters related to sound drivers of said casino-type game.

18. A method of authenticating a game data set as recited in claim 15 wherein said game-modifying data set includes a graphics modifying data set for modifying parameters related to graphically displayed images of the casino-type game.

19. A method of preparing a casino game data set capable of authentication, said method comprising the steps of:

- (a) providing a data set for a casino game;
- (b) computing a primary abbreviated bit string unique to the casino game data set;
- (c) encrypting the abbreviated bit string to provide a signature; and
- (d) storing the casino game data set and the signature.

20. A method of preparing a casino game data set as recited in claim 19 wherein said step (b) of computing is performed with a hash function to produce a hash value of the stored casino game data set, and wherein said primary abbreviated bit string comprises the hash value of the stored casino game data set.

21. A method of preparing a casino game data set as recited in claim 20 wherein the hash value comprises the message digest of the casino game data set.

22. A method of preparing a casino game data set as recited in claim 19 wherein said step (c) of encrypting is performed using a private encryption key.

23. A method of preparing a casino game data set as recited in claim 19 wherein said step (d) of storing the casino game data set and the signature includes storing the casino game data set and the signature in a mass storage device.

24. A method of preparing a casino game data set as recited in claim 23 wherein the mass storage device comprises a disk drive unit.

25. A method of preparing a casino game data set as recited in claim 23 wherein the mass storage device comprises a CD-ROM unit.

26. A method of preparing a casino game data set as recited in claim 23 wherein the mass storage device comprises a network storage system.

27. A method of authenticating a casino game data set of a casino type game having a signature encrypted from a primary abbreviated bit string computed from the casino game data set, said method comprising the steps of:

- (a) computing a complementary abbreviated bit string from the casino game data set;
- (b) decrypting the signature to recover the primary abbreviated bit string; and
- (c) comparing the primary and complementary abbreviated bit strings to determine whether the primary and complementary abbreviated bit strings match.

28. A method of authenticating a casino game data set as recited in claim 27 wherein said step (a) of computing is performed with a hash function to produce a hash value of the casino game data set, and wherein said complementary abbreviated bit string comprises the hash value of the casino game data set.

29. A method of authenticating a casino game data set as recited in claim 28 wherein the hash value comprises the message digest of the casino game data set.

30. A method of authenticating a casino game data set as recited in claim 27 wherein said step (b) of decrypting is performed using a public decryption key.

31. In an electronic gaming system including a main memory, a first storage means having a first authentication program stored therein, a second storage means having stored therein an anchor application including a second authentication program, and an anchor signature including an encrypted version of a unique primary abbreviated anchor bit string computed from said anchor application, and a third storage means having stored therein a game data set and a game signature including an encrypted version of a unique primary abbreviated game bit string computed from said game data set, a method of authenticating game data sets for implementing casino-type games, said method comprising the steps of:

- (a) loading said first authentication program stored in said first storage means to said main memory;
- (b) accessing said anchor application stored in said second storage means;
- (d) determining the validity of said anchor application using said first authentication program;
- (e) if said anchor application is invalid, prohibiting the loading of said anchor application into said main memory;
- (f) if said anchor application is valid, loading said anchor application into said main memory, accessing said anchor application stored in said third storage means, determining the validity of said anchor application using said first authentication program, if said anchor application is invalid, prohibiting the loading of said anchor application into said main memory, if said anchor application is valid, loading said anchor application into said main memory and processing instructions of said anchor application.

32. In an electronic gaming system as recited in claim 31 wherein said step of determining the validity of said anchor application using said first authentication program includes the steps of:

- computing a complementary abbreviated anchor bit string from said anchor application;
- decrypting said anchor signature to recover said primary abbreviated anchor bit string;

comparing said primary and complementary abbreviated anchor bit strings to determine whether said primary and complementary abbreviated anchor bit strings match.

33. In an electronic gaming system as recited in claim 31 wherein said step of determining the validity of said game data set using said second authentication program includes the steps of:

computing a complementary abbreviated game bit string from said game data set;

decrypting said game signature to recover said primary abbreviated game bit string;

comparing said primary and complementary abbreviated game bit strings to determine whether said primary and complementary abbreviated game bit strings match.

34. In an electronic gaming system as recited in claim 31 wherein said primary abbreviated anchor bit string is computed from said anchor application using a first hash function, and wherein said step of determining the validity of said anchor application using said first authentication program includes the steps of:

computing a complementary abbreviated anchor bit string from said anchor application using said first hash function;

decrypting said anchor signature to recover said primary abbreviated anchor bit string;

comparing said primary and complementary abbreviated anchor bit strings to determine whether said primary and complementary abbreviated anchor bit strings match.

35. In an electronic gaming system as recited in claim 34 wherein said primary abbreviated game bit string is computed from said game data set using a second hash function, and wherein said step of determining the validity of said game data set using said second authentication program includes the steps of:

computing a complementary abbreviated game bit string from said game data set using said second hash function;

decrypting said game signature to recover said primary abbreviated game bit string; and

comparing said primary and complementary abbreviated game bit strings to determine whether said primary and complementary abbreviated game bit strings match.

36. In an electronic gaming system as recited in claim 31 wherein said first storage means is an unalterable read only memory device.

37. In an electronic gaming system as recited in claim 31 wherein said second storage means is a mass storage device.

38. In an electronic gaming system as recited in claim 31 wherein said third storage means comprises a network storage system which is remote from the electronic gaming system.

39. In an electronic gaming system as recited in claim 31 wherein said electronic gaming system further includes a fourth storage means having stored therein a basic input/output operating system (BIOS) and wherein said first storage means further includes bootstrap code, an operating system, and operating system drivers stored therein, said method further comprising the steps of:

first loading said BIOS from said fourth storage means to said main memory; and

second loading said bootstrap code, said operating system, and said operating system drivers from said

first storage means to said main memory, wherein said steps of first and second loading are performed before performing said step of loading said first authentication program.

40. In an electronic gaming system as recited in claim 31 wherein said first storage means is an unalterable read only memory, said second storage means is a mass storage means, and said third storage means is a mass storage means.

41. In an electronic gaming system as recited in claim 31 wherein said step of determining the validity of said game data set using said second authentication program is repeatedly initiated in response to initiation of game play.

42. In an electronic gaming system as recited in claim 31 wherein said step of determining the validity of said game data set using said second authentication program is repeatedly initiated in response to the detection of a coin insert.

43. In an electronic gaming system as recited in claim 31 wherein said step of determining the validity of said game data set using said second authentication program is repeatedly initiated in response to the payout of coins or issuing of credit.

44. In an electronic gaming system as recited in claim 31 wherein said step of determining the validity of said game data set using said second authentication program is repeatedly initiated by a demand procedure activated remotely from the gaming system via a network.

45. In an electronic gaming system as recited in claim 31 wherein said step of determining the validity of said game data set using said second authentication program is repeatedly initiated by a demand procedure activated locally at the gaming system.

46. In an electronic gaming system as recited in claim 31 wherein said gaming system further includes a fourth storage means having stored therein a game modifying data set and a game modifying signature including an encrypted version of a unique primary abbreviated bit string computed from said game modifying data set, said method further comprising the steps of:

accessing said game modifying data set in said fourth storage means;

determining the validity of said game modifying data set using said second authentication program;

if said game modifying data set is invalid, prohibiting loading of said game modifying data set into said main memory; and

if said second game data set is valid, loading said game modifying data set into main memory.

47. In an electronic gaming system as recited in claim 31 wherein said game data set is a game-modifying data set which includes a money handler modifying data set for modifying parameters related to payout of coins and issuing of credit in the casino-type game.

48. In an electronic gaming system as recited in claim 31 wherein said game data set is a game-modifying data set which includes a sound driver modifying data set for modifying parameters related to sound drivers of said casino-type game.

49. In an electronic gaming system as recited in claim 31 wherein said game data set is a game-modifying data set which includes a graphics modifying data set for modifying parameters related to graphically displayed images of the casino-type game.

* * * * *